Techniques to Bootstrap a Verifiable Notion of Identity

Jan Lauinger

Technical University of Munich
TUM Department of Electrical and Computer Engineering
Associate Professorship of Embedded Systems and Internet of Things
Munich, April 2023
Who controls our digital identity today and how?
Single Sign-on (SSO)

1. Register at identity provider (IP) (e.g. Google)
2. Use IP to login at other services
   - You share your credentials only with one IP
   - Convenient as users only maintain one account
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google

Resource Owner
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google

2. Redirect to Google

Resource Owner

Identity Service
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google
2. Redirect to Google
3. Share Login Prompt

Resource Owner

Identity Service

To continue, Google will share your name, email address, language preference, and profile picture with eBay.
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google
2. Redirect to Google
3. Share Login Prompt
5. Enter credentials
6. Verify credentials

Resource Owner
Identity Service

To continue, Google will share your name, email address, language preference, and profile picture with eBay.
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google
2. Redirect to Google
3. Share Login Prompt
4. Enter credentials
5. Verify credentials
6. Access token (OAuth), ID token/JWT (OpenID)

To continue, Google will share your name, email address, language preference, and profile picture with eBay.
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google
2. Redirect to Google
3. Share Login Prompt
4. Identity Service
5. Enter credentials
6. Verify credentials
7. Access token (OAuth), ID token/JWT (OpenID)
8. Reload (+Token)

To continue, Google will share your name, email address, language preference, and profile picture with eBay.
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google
2. Redirect to Google
3. Share Login Prompt
4. Enter credentials
5. Verify credentials
6. Access token (OAuth), ID token/JWT (OpenID)
7. Authenticate with ID token
8. Reload (+Token)
9. Access token (OAuth), ID token/JWT (OpenID)

To continue, Google will share your name, email address, language preference, and profile picture with eBay.
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google
2. Redirect to Google
3. Share Login Prompt
4. Identity Service
5. Enter credentials
6. Verify credentials
7. Access token (OAuth), ID token/JWT (OpenID)
8. Reload (+Token)
9. Authenticate with ID token
9. Request resource with access token

To continue, Google will share your name, email address, language preference, and profile picture with eBay.
Open Authorization (OAuth 2.0) + OpenID

1. Login with Google
2. Redirect to Google
3. Share Login Prompt
4. Enter credentials
5. Verify credentials
6. Access token (OAuth), ID token/JWT (OpenID)
7. Authenticate with ID token
8. Request resource with access token
9. Share data
10. Show data + session cookie

Identity Service
Resource Service
Resource Owner
Problems

- **Control**: Fixed data policies
- **Verifiability**: Intransparent data access & data analytics
- **Security & privacy**: Data breaches & tracking
Problems

- **Control**: Fixed data policies
- **Verifiability**: Intransparent data access & data analytics
- **Security & privacy**: Data breaches & tracking

What we want instead:
- Control of identifiers, control of data policies
- Transparent access logs
- Verifiable policy-compliant computation
- No data breaches
- Provision of verifiable data
Question: Improving Centralized Infrastructure

Identity Service

Use my identity provider

Resource Owner

Resource Consumer

Resource Service
Question: Using Decentralized Approaches

Identity Service

Use my blockchain address

Resource Owner

Resource Service

IPFS

Resource Consumer
Bootstrapping a Decentralized Identity

Which techniques are required?
Wallets

- Custodial vs non-custodial wallets

Usenix 23: MFKDF for Fast, Flexible, Secure, & Practical Key Management
On-chain Accounts

- Registry contracts & Resolver contracts
- Privacy-preserving on-chain states & policies

Preprint 23: Zero-Knowledge Address Abstraction
Decentralized Storage Networks

- Store encrypted data

Usenix 16: Sieve; Usenix 20: Droplet
Decentralized Identity

Identity Service

Resource Owner

Use my blockchain address

Resource Consumer

IPFS

Resource Service
Taking the next step

What do we need on top of decentralized identity?
Decentralized Secret Management

Resource Owner

Identity Service

Secret Management Committee

IPFS

Resource Service

TCC 20: Can a public blockchain keep a secret?
Decentralized Access Control

VLDB 21: Calypso;
Can we achieve something even better, e.g. full data sovereignty?
Decentralized Secure Computation

Identity Service

Secret Management Committee

Compute Node Committee

Resource Service

Resource Owner

EuroS&P 22: SoK: privacy-preserving computing in the blockchain era
Decentralized Policy-compliant Computation

Identity Service

Resource Owner

Secret Management Committee

Compute Node Committee

Resource Consumer

IPFS

Resource Service

S&P 16: Hawk; EuroS&P 19: Ekiden;
EuroS&P 21: Publicly Auditable MPCaaS;
So far so good

- Control of identifiers, control of data policies
- Transparent access logs
- Verifiable policy-compliant computation
- No data breaches
- Provision of verifiable data
Something is missing

Is the data we provide authentic and trustworthy?

Resource Owner

IPFS

Resource Service
Ebay Seller KYC

Please share your proof of address & age.
Data Provenance Oracles

Oracle Verifier

Resource Owner

Trusted Data Provider

TLS three-party handshake

Kv

Kp

(Ks = Kp + Kv)

Ks

Get address & age

Request / Response execution

Commit(Response)

Disclose Kv

Compute & verify zk-proof
Ebay Seller KYC

- Address verified.
- Provision of verifiable data
Data Provenance Oracles

- Software based vs hardware based oracles, privacy-preserving oracles
- Server attested data vs verifier-based data attestation
- On-chain vs external oracles

TLSNotary; CCS 16: Town Crier; NDSS 18: TLS-N; CCS 20: DECO; S&P 21: Candid
If you are interested, please contact & monitor us

This year @EuroS&P 23: SoK Data Sovereignty

Github repository: web3knowledge

Upcoming work on TLS oracles…

Contact: jens.ernstberger@tum.de, jan.lauinger@tum.de
Thank you for listening

Questions?